SCAVENGER-CLASS QoS STRATEGY FOR DOS/WORM ATTACK MITIGATION
AT–A–GLANCE

DoS and worm attacks are exponentially increasing in frequency, complexity, and scope of damage.

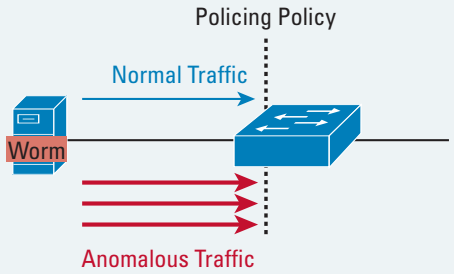
QoS tools and strategic designs can mitigate the effects of worms and keep critical applications available during DoS attacks.

One such strategy, referred to as Scavenger-class QoS, uses a two-step tactical approach to provide first- and second-order anomaly detection and reaction to DoS/worm attack-generated traffic.

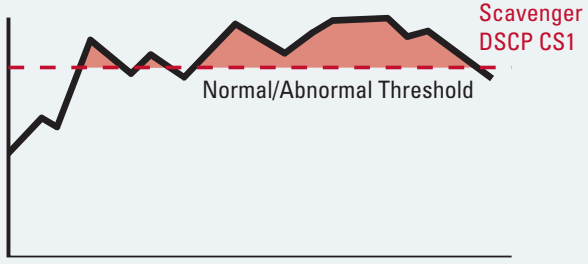
The first step in deploying Scavenger-class QoS is to profile applications to determine what constitutes a normal vs. abnormal flow (within a 95% confidence interval).

Application traffic exceeding this normal rate will be subject to first-order anomaly detection at the Campus Access-Edge, specifically: excess traffic will be marked down to Scavenger (DSCP CS1/8).

Note that anomalous traffic is not dropped or penalized at the edge; it is simply remarked.



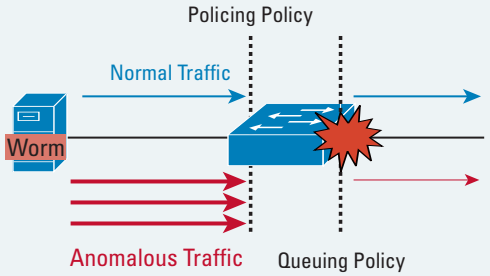
Only traffic in excess of the normal/abnormal threshold is remarked to Scavenger.



Campus Access-Edge policing policies are coupled with Scavenger-class queuing policies on the uplinks to the Campus Distribution Layer.

Queuing policies only engage when links are congested. Therefore, only if uplinks become congested, traffic begin to be dropped.

Anomalous traffic—previously marked to Scavenger—is dropped the most aggressively (only after all other traffic types have been fully-serviced).

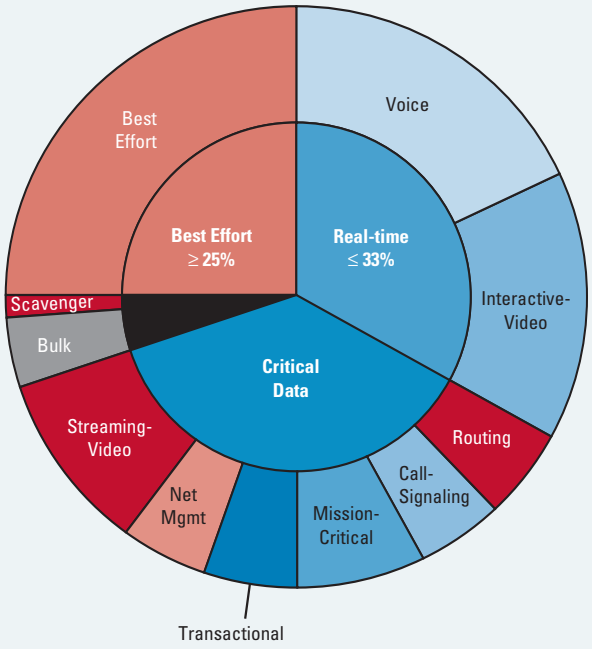


A key point of this strategy is that legitimate traffic flows that temporarily exceed thresholds are not penalized by Scavenger-class QoS.

Only sustained, abnormal streams generated simultaneously by multiple hosts (highly-indicative of DoS/worm attacks) are subject to aggressive dropping—and such dropping only occurs *after* legitimate traffic has beean fully-serviced.

The Campus uplinks are not the only points in the network infrastructure where congestion could occur. Typically WAN and VPN links are the first to congest.

Therefore, Scavenger-class "less-than-Best-Effort" queuing should be provisioned on all network devices in a consistent manner (according to hardware capabilities).



Thoroughly test QoS policies prior to production-network deployment.

It is critically important to recognize, that even when Scavenger-class QoS has been deployed end-to-end, this tactic only mitigates the effects of certain types of DoS/worm attacks, and does not prevent them or remove them entirely. Scavenger-class QoS is just one element of a comprehensive Cisco Self-Defending Networks (SDN) strategy.

204170.n_ETMG_AE_4.05